Math 220 Fall 2021, Lecture 3: Proofs

0.1. Proofs

Last time we have seen what a proposition is (a mathematical statement with a well-defined precise meaning). Now let's discuss about how to convince ourselves that propositions are true (or false). This is called **proof**.

What does, and what does not constitute a proof of a proposition? Here are two possible definitions:

Definition 0.1.1. An **informal proof** is a logical argument that convinces you that the proposition is true.

Definition 0.1.2. A **formal proof** is a piece of text (or code) that is structured according to certain rules (the rules of logic, but you can think of them as the rules of a game) and that concludes with the proposition. The rules are defined so precisely that a computer can check if a text adheres to them.

Both informal and formal proofs appear in real life. Formal proofs have become popular both in maths and CS since the 1960s, and in a way they are the gold standard. We are going to take a middle ground here:

Definition 0.1.3. A **proof** in our sense is an informal proof that a programmer (with some work) could turn into a formal proof.

It is this kind of proofs that we will be studying in this course.

So a proof is a logical argument. This means that it consists of "deduction steps": little steps in which you use something that you know to deduce something new from it.

Here are two examples:

Example 0.1.4. Let's say you know that any integer, when divided by 2, leaves either the remainder 0 or the remainder 1. (Strictly speaking, this needs to be proved, and we will actually prove it later.)

Now, you know that an odd integer cannot leave the remainder 0 (since that would make it even).

Thus you conclude that an odd integer must leave the remainder 1.

What you did here is a typical logical step: There are two options, but one of them is impossible, so the other must be the case.

Example 0.1.5. You know that an integer $n > 1$ is a prime number if and only if its only positive divisors are 1 and n. (Indeed, this is how "prime numbers" were defined.)

You thus conclude that an integer $n > 1$ that has a positive divisor other than 1 and n cannot be a prime. ("Prime" is shorthand for "prime number".)

From this, in turn, you conclude that 4 is not a prime, since 4 has a positive divisor other than 1 and 4 (namely, 2).

There were two logical steps here. In the first, you "turned" the definition of a prime around to obtain a criterion for being a non-prime. In the second, you applied the criterion to $n = 4$.

Here are some longer example proofs.

Proposition 0.1.6. The product of any two odd integers is odd.

Proof. Let a and b be two odd integers. We must show that ab is odd.

Since a is odd, the remainder that a leaves when divided by 2 is 1 (by the first example above). Let q be the quotient. Thus, $a = q \cdot 2 + 1$ (by the definition of quotient and remainder). We can rewrite this as $a = 2q + 1$.

Since b is odd, the remainder that b leaves when divided by 2 is 1 (by the first example above). Let s be the quotient. Thus, $b = s \cdot 2 + 1$ (by the definition of quotient and remainder). We can rewrite this as $b = 2s + 1$.

Now, because of $a = 2q + 1$ and $b = 2s + 1$, we obtain

$$ab = (2q + 1)(2s + 1) = 4qs + 2q + 2s + 1 = 2 \cdot (2qs + q + s) + 1.$$

Therefore, when dividing ab by 2 with remainder, we get the quotient $2qs + q + s$ and the remainder 1. In particular, the remainder is 1, so that ab is odd.

Forget that we fixed a and b. So we have shown that ab is odd whenever a and b are two odd integers. In other words, the product of any two odd integers is odd. This completes the proof. □

What have we used here? We have used the result of our first example. But we have used several more things:

- We have rewritten $q \cdot 2$ as $2q$. This relies on the **commutativity of multiplication**: the fact that $uv = vu$ for any integers u and v.
- When we multiplied out $(2q + 1)(2s + 1)$, we used the **distributivity** of integers: the fact that $(u + v) w = uw + vw$ and $u(v + w) = uv + uw$ for any integers u, v and w. We used a few more rules of addition and multiplication.
- Back in our first example, we implicitly used the **existence of quotient and remainder**. That is, we used the fact that any integer can be written as $q \cdot 2 + r$ for some integer q and some r that is either 0 or 1.
- At the end of our proof, we implicitly used the **uniqueness of quotient and remainder**. That is, we used the fact that for each integer n, there is **only one** pair of q and r such that $n = q \cdot 2 + r$. Indeed, the equality $ab = 2 \cdot$

$(2qs + q + s) + 1$ shows that $2qs + q + s$ and 1 form a "quotient-and-remainder pair" for ab in the sense that they "fit the bill" of what it means to be a quotient and a remainder. But assume that there would be another "quotient-and-remainder pair" for ab that would have a 0 instead of the 1. So ab would be simultaneously $2 \cdot (\text{something}) + 1$ and $2 \cdot (\text{something else}) + 0$. Then, ab would be even, not odd.

Our use of the uniqueness was implicit in our use of the definite article ("the") when we said "the quotient" and "the remainder".

What else did we do in the above proof? We made several logical deduction steps. At the beginning of the proof, we introduced two variables (a and b), by saying "Let a and b be two odd integers". Any statement from that moment on was a statement about a and b; so a and b are part of its "context". At the end of the proof, we "un-introduced" these variables, by saying "Forget that we fixed a and b". In the second-to-last sentence, we recovered the claim of the proposition ("the product of any two odd integers is odd"). The last sentence ("This completes the proof") is a traditional way of giving structure to the text; synonyms for it are "This completes the proof" or "This proves the proposition" or "The proposition is thus/now proved" or "QED". Alternatively, the $\square$ symbol is often used for the same purpose (i.e., to mark the end of a proof).

Here is another example of a proof:

Proposition 0.1.7. There are infinitely many primes. (Recall that "prime" means "prime number".)

This is a classical result from Euclid's Elements.

First, let me restate it in a more formal fashion. What does "infinitely many" mean? It means that if you give me any finite list of primes, I can find you another prime. ("Finite" in this case means "has a length that is an integer".) In other words, it means the following:

Proposition 0.1.8. (A concrete statement of the preceding proposition:)
If $p_1, p_2, \ldots, p_k$ are finitely many primes (with k being an integer), then there exists a prime p that equals none of them.

Proof. Let $p_1, p_2, \ldots, p_k$ be finitely many primes. Set

$$N = p_1 p_2 \cdots p_k + 1.$$

We know that N is an integer and $N > 1$. Therefore, I claim the following:

Claim 1: This integer N must be divisible by some prime.

[*Proof of Claim 1:* Consider the positive divisors of N. Let d be the **smallest** positive divisor of N that is greater than 1 (note that such a divisor exists, since

N is a such). Then, d is prime, because any positive divisor of d other than 1 and d would have to be an even-smaller positive divisor of N (distinct from 1) than d, which however is impossible because d was already the smallest one. Thus, N is divisible by a prime (namely, d). This proves Claim 1.]

Claim 1 shows that N is divisible by some prime. In other words, there exists a prime p which divides N. Consider this p.

Claim 2: This prime p equals none of $p_1, p_2, \ldots, p_k$.

[*Proof of Claim 2:* Assume that $p = p_i$ for some i. Thus, p divides $p_1 p_2 \cdots p_k$. In other words, $p_1 p_2 \cdots p_k = pa$ for some integer a. So $N = \underbrace{p_1 p_2 \cdots p_k}_{=pa} + 1 = pa + 1$. This shows that N leaves the remainder 1 when divided by p. Thus, N is not divisible by p. But N is divisible by p, as we know! So we got a contradiction. Thus, our assumption (that $p = p_i$ for some i) cannot be true. So we have shown that p is not equal to any of $p_1, p_2, \ldots, p_k$. In other words, p equals none of $p_1, p_2, \ldots, p_k$. This proves Claim 2.]

Claim 2 shows that there exists a prime p that equals none of $p_1, p_2, \ldots, p_k$. This proves the proposition. □

Example 0.1.9. Let us see how this proof works if my list $(p_1, p_2, \ldots, p_k)$ is $(2, 7)$. According to the proof, I can now find a new prime by setting

$$N = p_1 p_2 \cdots p_k + 1 = 2 \cdot 7 + 1 = 15$$

and picking a prime p that divides N. How do we find p ? We take the smallest positive divisor of N that is greater than 1 and call it p. So $p = 3$. And indeed, 3 is a prime that equals none of $2, 7$.

Continuing this method with the list $(2, 7, 3)$, we obtain $(2, 7, 3, 43)$, and so on, obtaining $(2, 7, 3, 43, 13, 53, 5, 6221\,671, \ldots)$.